Electronic Version
Stylesheet Version v1.1.1

IMPLEMENTING NONREPUDIATION AND AUDIT USING AUTHENTICATION ASSERTIONS AND KEY SERVERS

Abstract

A communication system (410) wherewith sources (414) and targets (416) employ a key server (420) to exchange transactions (424). A first request to the key server includes a source assertion (422) from an authentication authority (418), and optionally a key (430). The key server provides a transaction ID (428), and the key if not already provided, in reply to this request. The key server stores the transaction ID and source assertion. The source encrypts the transaction and sends it with the transaction ID to the targets. A second request to the key server includes a target assertion and the transaction ID. The key server provides the key in reply to this request. The key server also stores the target assertion in association with the transaction ID. The respective assertions then establish the source and targets of the transaction in a manner that cannot plausibly be repudiated.